

Aircraft Developer Looks to Modernize Storage of Sensitive Data

**CURTISS-
WRIGHT**
DEFENSE SOLUTIONS


Challenge

- SWaP-constrained fixed-wing aircraft
- Multiple networks requiring data storage
- Difficulties integrating encryption systems

Solution

- Rugged, SWaP-optimized NAS file server
- Pre-boot execution from single location
- Built-in AES256-bit encryption

Results

- Increase in available onboard space
- Reduced time spent maintaining systems
- Met schedule with a ready-to-deploy system

Challenge

Intelligence, Surveillance, and Reconnaissance (ISR) aircraft carry multiple mission and sensor networks in order to conduct both surface and maritime missions. These networks create a lot of data that must be securely stored and then removed for debriefings, requiring a rugged storage solution that can keep up with the incoming data and withstand challenging environmental conditions. Tasked with modernizing the systems aboard fixed-wing ISR aircraft, a leading C5ISR system integrator reached out to Curtiss-Wright in search of a network attached storage (NAS) server that would bring the aging fleet up to date.

The upgrades to the existing aircraft were essential to enhance capabilities and increase the aircraft's effectiveness, and upgrading the data transfer and communications to

a state-of-the-art system was essential to accomplishing that goal. The key criteria in their search was a system that could be modernized over the previously used storage, while greatly reducing the overall footprint and weight within the aircraft.

The data that was stored on the device would also need to be encrypted. The integrator previously had difficulty using storage devices that needed third-party encryptors to be integrated. This would often result in longer than expected timelines in the integration period and delayed deployment. Given that the schedule surrounding the platform upgrades was also relatively tight, as the fleet of aircraft needed to return to service, the system integrator needed a solution that would come as a package.



**CURTISS-
WRIGHT**

Curtiss-Wright DTS1
Rugged Network Attached File Server

Another challenge that the integrator faced was the decentralization of all the networks running on the aircraft. This often meant that updating software on all the onboard mission and sensor systems required individual maintenance, which would prolong the time the aircraft were inoperable. In an effort to reduce ground time, the integrator was looking for a way to implement a remote boot of the network clients aboard the aircraft to reduce the software maintenance effort.

Solution

To fulfill their need, Curtiss-Wright recommended the [DTS1 rugged network attached file server](#) for the ISR aircraft. The DTS1 allows any network client on the aircraft to save a file on the device or retrieve a file from it. In addition to Network File System (NFS), Common Internet File System (CIFS), File Transfer Protocol (FTP), and HTTP protocols, the DTS1 also supports the ability to boot network clients with Preboot Execution Environment (PXE). This enables the system integrator and the ISR aircraft operator to load operating systems (OS) and application code on the DTS1's removable memory cartridge (RMC). Each time the system boots, each network client uses PXE to obtain its OS and application program from the DTS1, thus eliminating separate storage drives in each of the clients. More importantly, the client software is updated easily whenever required.

The platform also required the [data-at-rest \(DAR\) be encrypted](#). While the DTS1 offers an option for two distinct layers of encryption (hardware and software), the system integrator opted to only have the hardware layer included. The hardware layer is full disk encryption (HWFDE) using an AES256-bit FIPS 140-2 certified ASIC. While not a requirement at this time for this platform, the additional software layer could be added later if requirements change.

The small size, weight, and power (SWaP) consumption was also a big factor in choosing the DTS1. The DTS1 is packaged in a lightweight, compact chassis that measures just 1.5 inches tall and less than 48 inches cubed. When

equipped with a 2 TB (up to 8 TB supported) removable memory cartridge (RMC), the DTS1 weighs in at less than 4 lbs and uses less than 18 watts of power. This unique combination eliminated the system integrator's potential dilemma of compromising either encryption or SWaP. The use of the RMC also provides the customer with a durable, high-insertion cycle connector designed for 100,000 removals/insertions, ensuring that the module can be safely removed for post-mission analysis and playback for a program long life expectancy.

Results

Choosing the DTS1 provided the system integrator and customer everything they required to modernize the ISR aircraft fleet. Not only are the DTS1 units capable of acquiring and storing the multiple mission and sensor networks built into the platform, but the device is able to do so while keeping SWaP to a minimum. By using a SWaP-optimized solution, the system integrator was able to utilize the excess space for additional mission resources.

By utilizing the PXE boot feature available with the DTS1, the integrator provided the customer with an easy-to-maintain platform. Whenever an update is needed, the customer can simply upload the updates to the RMC and insert it into the DTS1. The next time the system is turned on, the DTS1 deploys the updates to all connected network clients. The integrator has already seen a decrease in time needed for system maintenance and an increase in time the fleet can be mission ready.

Designed to provide encryption out of the box, the DTS1 was also a good choice for the developer given the tight program schedule. Curtiss-Wright was able to provide the system integrator with a built-in data encryption solution so they didn't need to develop or implement a separate encryption solution, ensuring the timely delivery needed to deploy the updated aircraft.